RECOMMENDED STATE GOVERNMENT PROTECTIVE MEASURES

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist Yes	Checklist No	GREEN-LOW (LOW RISK of terrorist attack) Recommended Protective Measures:
G-1			Disseminate the GREEN advisory and share pertinent information related to the Homeland Security Threat Condition with state agencies/offices and government officials.
G-2			Identify critical facilities that may need protection. Budget for physical security measures.
G-3			Develop, review and/or update Emergency Response plans. Conduct training, seminars, workshops and exercises using the emergency response plans.
G-4			Develop or review, coordinate and exercise Mutual Aid agreements with other jurisdictions for use during emergencies.
G-5			Be alert to suspicious activities and / or individuals and report it to proper authorities or law enforcement agencies. Be suspicious of person(s) taking photographs of critical facilities, asking detailed questions about physical security or dressed inappropriately for weather conditions.
G-6			Routine operations without security stipulations are allowable. Possible security recommendations or considerations include: • Reviewing physical security precautions to minimize the risk of theft, unauthorized entry or destruction of property. • Providing access control and locking of high security areas. • Marking all security keys with "Do Not Duplicate."
G-7			Continue to include safety and common sense practices in daily routines. Conduct emergency preparedness training for employees. Provide emergency preparedness information to employees via paycheck inserts, tips, newsletters, articles and posters. Obtain copy of Terrorism: Preparing for the Unexpected brochure from your local Red Cross chapter. Obtain a copy of the United for a Stronger America: Citizens' Preparedness Guide from the National Crime Prevention Council (http://www.weprevent.org). Additional information on preparedness is available at Ready.Gov or by calling 1-800-BE-READY (1-800-237-3239).
G-8			Provide training on Homeland Security Advisory System ("HSAS") and physical security precautions.
G-9			Review staffing of emergency management and response functions. Recruit and train volunteers to augment full time staff, as appropriate. Contact Citizen Corps for potential volunteers (http://www.citizencorps.gov/).
G-10			Encourage employees to take Emergency Management, Red Cross first aid and Cardio-Pulmonary Resuscitation (CPR)/Automated External Defibrillator (AED) training.
G-11			Conduct routine inventories of emergency supplies and medical aid kits. Update and restock as required.
G-12			Encourage programs for employee immunizations and preventative health care.
G-13			Develop a communications plan for emergency response and key personnel.
G-14			Develop or review agency Continuity of Operations Plan.
G-15			Governor or EMD issues public information release, as appropriate.

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist Yes	Checklist No	BLUE- GUARDED (GENERAL RISK of terrorist attack) Recommended Protective Measures:
B-1			Disseminate the BLUE advisory and share pertinent information related to the Homeland Security Threat Condition with state agencies/offices and government officials.
B-2			Continue all measures listed in Homeland Security Threat Condition GREEN Advisory.
B-3			Review all applicable emergency plans (e.g. Emergency Operations Plan, Standard Operating Procedures (SOP) / Standard Operating Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc., as applicable). Each department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.
B-4			Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include: • Issuing employee picture ID badges. • Conducting background checks on employees, if authorized. • Installing surveillance cameras in vulnerable areas. • Providing a back-up power source for critical functions. • Installing an alarm system for critical buildings, doors or offices. • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature. • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.
B-5			Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.
B-6			Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.
B-7			Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.
B-8			Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.
B-9			Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.
B-10			Evaluate information available on public websites that could compromise security.

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist Yes	Checklist No	YELLOW – ELEVATED (SIGNIFICANT RISK of terrorist attack) Recommended Protective Measures:
Y-1			Disseminate the YELLOW advisory and share pertinent information related to the Homeland Security Threat Condition with state agencies/offices and government officials.
Y-2			Continue all measures listed in the Homeland Security Threat Condition GREEN and BLUE Advisories.
Y-3			Implement critical infrastructure facility security plans, as appropriate. Assess potential terrorist targets and develop additional plans, if necessary, to counteract an attack. Conduct additional vulnerability assessments of each critical facility and government building, as necessary. Assess the consequence of loss and assign a priority for their protection. Meet with appropriate representatives of critical infrastructure facilities to review contingency and evacuation plans and brief employees, as appropriate. Possible security recommendations or considerations include: • Increasing spot checks of specific high-risk targets / facilities. At the beginning and end of each work shift, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious or unattended packages. • Not leaving emergency response vehicles unattended. If it is necessary to leave the vehicle, lock it and check the vehicle and its chassis underside before opening the door and starting the engine. • Checking all deliveries to facilities.
Y-4			Check recall roster and recall processes for accuracy. Consider alternative work schedules of operational and staff personnel if the situation escalates. Include plans to maximize staffing and response capabilities with defined work / rest cycles.
Y-5			Identify any planned community events where a large attendance is anticipated. Consult with event organizers regarding contingency plans, security awareness, and site accessibility and control. Consider recommendations to cancel the event if warranted by the current situation.
Y-6			Increase the frequency of backups for critical information systems and review availability of technical support: e.g. systems programmers, technical personnel, redundancy of equipment, off-site storage of critical data, stockpile of critical spare parts, off-site data recovery , etc.
Y-7			Keep the public informed on current Homeland Security Threat Conditions and advisories.

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist Yes	Checklist No	ORANGE – HIGH (HIGH RISK of terrorist attack) Recommended Protective Measures:
O-1			Disseminate the ORANGE advisory and share pertinent information related to the Homeland Security Threat Condition with state agencies/offices and government officials.
O-2			Continue all measures listed in the Homeland Security Threat Condition GREEN, BLUE and YELLOW Advisories.
O-3			Activate the agency's Emergency Operations Center (EOC) for an initial situation briefing of EOC staff and government officials. Following the initial briefing maintain staffing, as appropriate.
O-4			Place all emergency management and specialized response teams on full alert status, as appropriate.
O-5			Review critical infrastructure and facility security plans and adjust accordingly. Possible security recommendations or considerations include: • Limiting access points to critical infrastructure facilities to the absolute minimum, and strictly enforcing entry control procedures. Locking all exterior doors except the main facility entrance(s). Identifying and protecting all designated vulnerable points. • Searching all suitcases, briefcases, packages, etc. brought into a facility. • Checking all visitors' purpose, intent and identification. Checking that contractors have valid work orders outlining tasks to be performed within the secured facility. Requiring a visitor's sign-in log with information from their identification. Escorting visitors when they are in the facility, until they leave. Checking where the visitors were or worked to assure nothing is amiss or left behind. • Keeping critical response vehicles in a secure area or in an indoor facility. Keeping garage doors closed except for bona fide needs. • Enforcing parking of vehicles away from sensitive buildings. Erecting barriers and obstacles to control the flow of traffic, as appropriate. Visually inspecting the interior and undercarriage of vehicles entering parking lots and terraces. • Increasing defensive perimeters around key structures and events. Increasing security patrols around critical infrastructure facilities. Contacting allied government agencies within the jurisdiction and advising them of the need for increased security and awareness. • Coordinating closure of public roads and facilities that might make critical facilities more vulnerable to attack.
O-6			Determine if personal protective equipment (PPE) and specialized response equipment has been checked, issued, and readily available for deployment, if applicable.
O-7			Suspend public tours of critical infrastructure facilities. Limit access to computer facilities.
O-8			Increase monitoring of computer and network intrusion detection systems and security monitoring systems. Determine if sufficient technical resources are available to respond to and mitigate a cyber attack.

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist Yes	Checklist No	RED – SEVERE (SEVERE RISK of terrorist attack) Recommended Protective Measures:
R-1			Disseminate the RED advisory and share pertinent information related to the Homeland Security Threat Condition with state agencies/offices and government officials.
R-2			Continue all measures listed in the Homeland Security Threat Condition GREEN, BLUE, YELLOW and ORANGE Advisories.
R-3			Request the Governor proclaim a state of emergency if attack is specific to Washington or if required to support a state requiring Mutual Aid, as appropriate.
R-4			Staff State Emergency Operations Center (EOC) or Command Post on a 24-hour basis. Provide security for this facility.
R-5			Review critical infrastructure and facility security plans and adjust accordingly. Possible security recommendations or considerations include: • Making a positive identification of all vehicles located or operating within operational or mission support areas. • Making frequent checks of the exterior of critical facilities and begin spot checks of lower risk targets. Consider placing a security watch at all sensitive facilities 24-hours a day until the Homeland Security Threat Condition level has diminished. • Deliveries to critical facilities should not be accepted unless approved by supervisory staff. All deliveries should not be opened inside of the facility, and minimal personnel should be in the immediate area when the package is opened.
R-6			Consider releasing non-critical function personnel.
R-7			EOC has 24-hour access to the agency/office Principal Executive Officer (e.g. Secretary, Director, elected official) or their designated alternate.
R-8			Brief all EOC, government and first response personnel on critical facility evacuation routes and contingency communications plans. Provide direction regarding what equipment and supplies should be taken in the event of an evacuation.
R-9			Conduct welfare checks of government personnel and facilities throughout the day and night.
R-10			Activate, or place on high alert specialized response teams / personnel; e.g. HAZMAT, EMS, SWAT, Crisis Counseling, etc.
R-11			Be prepared to control access routes serving critical infrastructure facilities and evacuation routes.
R-12			Maintain communications with, and provide security for hospitals and critical medical facilities, if appropriate.
R-13			Stress the possibility of a secondary attack against first responders.
R-14			Assemble trained volunteers including: Community Emergency Response Teams ("CERT"), Community Policing ("COP") Teams, Amateur Radio Emergency Services ("ARES") teams.
R-15			Implement Mutual Aid agreements, as required.
R-16			Provide security for personnel dispatched to repair or restore damaged facilities and systems.